UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/566,943	02/03/2006	Takatoshi Kato	062807-0316	2588

20277 7590 11/25/2008
MCDERMOTT WILL & EMERY LLP
600 13TH STREET, N.W.
WASHINGTON, DC 20005-3096

EXAMINER	
VU, PHY ANH TRAN	

ART UNIT	PAPER NUMBER
4148	

MAIL DATE	DELIVERY MODE
11/25/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/566,943	**Applicant(s)** KATO ET AL.	
	Examiner PHY ANH VU	**Art Unit** 4148	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 February 2006*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03 February 2006* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date
2/03/2006,9/5/2007,9/17/2007,3/25/2008,4/24/200899 9/29/2008 and 11/19/2008.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. The instant application having Application No. 10/566,943 filed on 2/03/2006 is presented for examination by the examiner.

Claims 1-16 are pending and claims 17-21 are cancelled.

Oath/Declaration

2. The applicant's oath/declaration has been reviewed by the examiner and is found to conform to the requirements prescribed in **37 C.F.R. 1.63.**

Information Disclosure Statement

3. The information disclosure statement (IDS) submitted on 2/3/2006, 9/5/2007, 9/17/2007, 3/25/2008, 4/24/2008, and 9/29/2008 are in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Objections

4. **Claim 3** is objected to because of the following informalities: It appears that there is an extra "wherein" on line 1 of claim 3.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. **Claims 5** is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 5 recites "The remote access system according to claim 1 wherein the storage medium to the non-volatile memory area;" This is vague and also incomplete.

For the purpose of examination, examiner will interpret this as the non-volatile memory area is a component of the smart card.

Double Patenting

A rejection based on double patenting of the "same invention" type finds its support in the language of 35 U.S.C. 101 which states that "whoever invents or discovers any new and useful process ... may obtain a patent therefor ..." (Emphasis added). Thus, the term "same invention," in this context, means an invention drawn to identical subject matter. See *Miller v. Eagle Mfg. Co.*, 151 U.S. 186 (1894); *In re Ockert*, 245 F.2d 467, 114 USPQ 330 (CCPA 1957); and *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970).

A statutory type (35 U.S.C. 101) double patenting rejection can be overcome by canceling or amending the conflicting claims so they are no longer coextensive in scope. The filing of a terminal disclaimer cannot overcome a double patenting rejection based upon 35 U.S.C. 101.

Instant Application	Copending Application 11/979,123
(claim 1)	(claim 1)
a remote access system comprising:	a remote access system comprising:
a server ;	a server ;
a client;	a client;
device for conducting remote access to the server via a communication channel constituted between the client device and the server; and	device for conducting remote access to the server via a communication channel constituted between the client device and the server; and
a storage medium comprising an anti-tampering memory area for storing authentication information to constitute the communication channel and conduct the remote access, and a non-volatile memory area, the storage medium being connected to the client device	a storage medium comprising an anti-tampering memory area for storing authentication information to constitute the communication channel and conduct the remote access, and a non-volatile memory area, the storage medium being connected to the client device
wherein	wherein
the storage medium comprises a common interface to be used by the client device to access the anti-tampering memory area and the non-volatile memory area, and	the storage medium comprises a common interface to be used by the client device to access the anti-tampering memory area and the non-volatile memory area, and
the client device;	the client device;
accesses the anti-tampering memory area and the non-volatile memory area via the common interface in the storage medium;	accesses the anti-tampering memory area and the non-volatile memory area via the common interface in the storage medium;
constitutes the communication channel between the client device and the server by using a program stored in the non-volatile memory area and the authentication information stored in the anti-tampering memory area; and	constitutes the communication channel between the client device and the server by using a program stored in the non-volatile memory area and the authentication information stored in the anti-tampering memory area; and
conducts remote access to the server via the communication channel.	conducts remote access to the server via the communication channel.

Claims 1 of the instant application is compared to claims 1 of the copending application 11/979,123 in the above table.

Examiner Notes

6. Examiner cites particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that, in preparing responses, the applicant fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 5, 9-10, 12 are rejected under 35 U.S.C. 102(e) as being anticipated by **Fraser (US 6,895,502 B1)**.

Regarding claim 1, Fraser discloses a remote access system comprising:

a server (*Fig. 1, element 12; Col 5, lines 8, 58; host computer or server*);

a client (*Fig. 1, element 14*; *Col 5, line 8; Col 8, line 38, client computer*);

device for conducting remote access to the server via a communication channel constituted between the client device and the server (*Fig. 1, element 15*; *Col 8, lines 38-43, LAN or WAN; Internet*); and

a storage medium comprising an anti-tampering memory area for storing authentication information to constitute the communication channel and conduct the remote access *(Col 9, lines 7-9, 37-54; Col 11, lines 25-27; Nonvolatile storage (e.g., hard disk) and tamper-resistant packaging, which corresponds to anti-tampering memory area that contains private key of the client user*); and a non-volatile memory area (Col 8, line 64-67; *Col 9, lines1-6,the program memory stores program which is executed in ROM to protect from unauthorized modification*), the storage medium being connected to the client device (*Fig. 1, lines 12-16; wherein the smart card which corresponds to the storage medium is being connected to the client computer via a communication medium or pathway*),

wherein

the storage medium comprises a common interface to be used by the client device to access the anti-tampering memory area and the non-volatile memory area (*Fig 1, element 20; Col 9, lines 55-60; Reader*)

and the client device (*Fig. 1, element 14; Col 7, lines 30-31; Col 8, line 38; terminal or computer*) accesses the anti-tampering memory area and the non-volatile memory area via the common interface in the storage medium (*Fig 1, element 20; Col 9, lines 55-60; Reader*)

constitutes the communication channel between the client device and the server by using a program stored in the non-volatile memory area and the authentication information stored in the anti-tampering memory area (*Col 12, lines 4-20, wherein a communication channel is established between server and client device*)

conducts remote access to the server via the communication channel (*Fig. 1, element 15; Col 8, lines 38-43; internet*).

Regarding claim 5, as mentioned under the U.S.C 112, 2nd paragraph rejection above Fraser also discloses the remote access system according to claim 1, wherein the storage medium to the non-volatile memory area is a component of the smart card (*Fig 1, element 18; Col 8, lines 52-53; Col 9, lines 7-9*) wherein the client device stores temporary data generated when executing a program in the client device in the storage medium (*Col 8, lines 59-63; RAM*).

Regarding claim 9, Fraser discloses a remote access system comprising:

a server (*Fig. 1, element 12; Col 5, lines 8, 58; host computer or server*):

a client device for conducting remote access to the server via a communication channel constituted between the client device and the server (*Fig. 1, elements 14, 15*; Col 5, lines 8; *Col 8, lines 38-43, LAN or WAN; Internet*);

a storage medium comprising an anti-tampering memory area for storing authentication information to constitute the communication channel and conduct the remote access *(Col 9, lines 37-54; Col 11, lines 25-27; tamper-resistant packaging, which corresponds to anti-tampering* *memory area that contains private key of the client user*); and a non-volatile memory area for storing a boot program to be executed when the client device is driven (*Col 12, lines 12-15*), wherein the storage medium comprises a common interface to be used by the client device to access the anti-tampering memory area and the non-volatile memory area (*Fig 1, element 20; Col 9, lines 55-60; Reader*)

and the client device (*Fig. 1, element 14; Col 7, lines 30-31; Col 8, line 38; terminal or computer*)

accesses the anti-tampering memory area and the non-volatile memory area via the common interface of the storage medium (*Fig 1, element 20; Col 9, lines 55-60; Reader*);

starts a driving process by executing the boot program stored in the storage medium (*Col 12, lines 12-20; Col 15, lines 6-21 wherein boot program from the smartcard is executed*) ;

constitutes the communication channel between the client device and the server by using a program stored in the non-volatile memory area and the authentication information stored in the anti-tampering memory area after the client device is driven (*Col 12, lines 4-20*, *wherein a communication channel is established between server and client device*); and

conducts remote access to the server via the communication channel (*Fig. 1, element 15; Col 8, lines 38-43; internet*).

Regarding claim 10, Fraser also discloses the remote access system according to claim 9, wherein when access to the non-volatile memory area and access to the anti-tampering memory area conducted via the common interface in the storage medium compete with each other, the client device controls the competition (*Col 6, lines 40-53, wherein in order for the client device to access the server resources, the client device is required to provide authorized information i.e., private key, which is retrieved from the anti-tampering memory by the client device. This implies that the client device has the capabilities to control which memory areas to access first in order to get the authorized information)*

Regarding claim 12, Fraser discloses the remote access system according to claim 9, wherein the client device comprises a display means (*Fig 1, element 22; Col 9, lines 23-36, display unit*); and a screen view is displayed on the display means to request a user to input authentication information required when constituting the communication channel (*Fig 2, element 51; Col 12, lines 23-28, 47-50, 53-55, 61-64; Col 13, lines 30-35; wherein, the system prompts user to enter identification information and confirmation that user did make the request, which implies that there is a screen view, where user can visibly see the prompts and able to input the information the system requires).*

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. **Claims 2-4** are rejected under 35 U.S.C. 103(a) as being unpatentable over Fraser.

Regarding claim 2, Fraser discloses the remote access system according to claim 1, wherein when access to the non-volatile memory area and access to the anti-tampering memory area conducted via the common interface in the storage medium compete with each other the client device controls the competition (*Col 6, lines 40-53, wherein client device accesses a resource. This implies that the client device has the capabilities to control which area of the resource it accesses first)*

It is also obvious to one of ordinary skill in the art that when there are conflicting accesses to a common resource in a computer system that does not support parallel accesses, the computer system must have a mechanism that lines up the requests to access the resource, so that only one request will be executed at a time. Request with higher priority will be given access first.

One of ordinary skill in the art at the time the invention was made would have been motivated to incorporate this feature into the teachings of Fraser because it would provide for higher security in accessing the host computer or server (Col 4, lines 64-67; Col 5, lines 1-4).

Regarding claim 3, Fraser also discloses the remote access system according to claim 2, wherein the client device controls the competition by conducting access to the non-volatile memory area and access to the anti-tampering memory area to be conducted via the common interface in the storage medium in a predetermined order (*Col 6, lines 40-53; Col 8, lines 64-67; Col 9, lines 1-9, wherein since the client device has control over the competition, and authentication information is needed from the anti-tampering area to authenticate the client* *device before access to the server resource is given. Clearly, access to the anti-tampering area has priority over access to the non-volatile area, thus the anti-tampering area will be accessed first. This shows the predetermined order of accessing to the memory areas of the storage medium)*

It is also obvious to one of ordinary skill in the art that when there are conflicting accesses to a common resource in a computer system that does not support parallel accesses, the computer system must have a mechanism that lines up the requests to access the resource, so that only one request will be executed at a time. Request with higher priority will be given access first.

One of ordinary skill in the art at the time the invention was made would have been motivated to incorporate this feature into the teachings of Fraser because it would provide for higher security in accessing the host computer or server (Col 4, lines 64-67; Col 5, lines 1-4).

Regarding claim 4, Fraser also discloses the remote access system according to claim 3, wherein the client device controls the competition by executing access to the anti-tampering memory area to be conducted via the common interface in the storage medium in preference to access to the non-volatile memory area (*Col 6, lines 40-53; Col 8, lines 64-67; Col 9, lines 1-9, 37-54, wherein in order for the client device to have access to the server resources, the client device must first be authorized using the authentication information stored in the anti-tampering area. This clearly shows that access to the anti-tampering memory area has higher priority than* *access to the non-volatile area, thus access to the anti-tampering should be accessed in preference to access to the non-volatile area)*

It is also obvious to one of ordinary skill in the art that when there are conflicting accesses to a common resource in a computer system that does not support parallel accesses, the computer system must have a mechanism that lines up the requests to access the resource, so that only one request will be executed at a time. Request with higher priority will be given access first.

One of ordinary skill in the art at the time the invention was made would have been motivated to incorporate this feature into the teachings of Fraser because it would provide for higher security in accessing the host computer or server (Col 4, lines 64-67; Col 5, lines 1-4).

10. **Claim 6** is rejected under 35 U.S.C. 103(a) as being unpatentable over Fraser, and further in view of Knegendorf et al (US 2003/0040929 A1, hereinafter Knegendorf).

Regarding claim 6, **Fraser discloses** the remote access system according to claim 1, wherein the non-volatile memory area in the storage medium is configured so as to be able to be accessed by the client device faster than the anti-tampering memory area (*Col 9, lines 1-9, wherein accessing to ROM is faster than accessing to anti-tampering memory area i.e. hard disk*)

Fraser does not disclose the storage medium retains a copy of the authentication information stored in the anti-tampering area, in the non-volatile memory area in the storage medium and the client device utilizes the copied authentication information instead of the authentication information stored in the anti-tampering area.

However, Knegendorf discloses copying content data from one storage area (*nonvolatile*) to another storage area (*volatile*) and the user utilizes the copied content data (*volatile*) instead of the original content data (*[0145], this is because storing data in a volatile memory makes access to data faster). It is also known in the art to retain a copy of the information in the non-volatile area because accessing data from a faster volatile memory involves the risk of information loss in case of a power outage or volatile memory failure, so it is common practice to keep a copy of data in a non-volatile memory while the information is accessed from the faster volatile memory)*

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify this feature of Knegendorf into the teachings of Fraser because it would provide for faster access to the information (*[0145])*.

11. **Claim 7** is rejected under 35 U.S.C. 103(a) as being unpatentable over Fraser, and further in view of Ugajin (US 5,652,892).

Regarding claim 7, Fraser discloses the remote access system according to claim 1 (*Fig. 1, remote access system*),

Fraser does not disclose a controller connected to the server and the client device to manage a power supply of the server, wherein the client device accesses the controller and conducts power supply management of the server to be subject to the remote access.

However, Ugajin discloses a controller connected to the server and the client device to manage a power supply of the server (*Figs. 9 & 10*), wherein the client device accesses the controller and conducts power supply management of the server to be subject to the remote access (*Figs. 9 & 10; Col 6, lines 28-34, wherein the client device controls the power source of the server*).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Ugajin into the teachings of Fraser because it would provide for a remote power source control method and apparatus capable of controlling remote power sources independently of network architectures. (*Col 1, lines 60-63)*

Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Fraser, and further in view of Gould et al (US 6,920,561 B1, hereinafter Gould).

Regarding claim 8, Fraser discloses the remote access system according to claim 1, wherein the storage medium is connected to the client device (*Fig. 1, lines 12-16; wherein the smartcard which corresponds to the storage medium is being connected to the client computer via a communication medium or pathway*),

client device for conducting remote access to the server via a communication channel constituted between the client device and the server (*Fig. 1, elements 14, 15*; Col 5, lines 8; *Col 8, lines 38-43, LAN or WAN; Internet*);

remote access conducted by the client device using the communication channel (*Fig. 1, element 15; Col 8, lines 38-43; internet*).

Fraser does not disclose the client device deletes information concerning the remote access.

However, Gould discloses the client device deletes information concerning the remote access (*Col 5, lines 44-47, wherein, the user credentials are deleted by the client device at the end of the session, which implies that communication is finished, and the connection between the client device and storage medium is canceled*).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Gould into the teachings of Fraser because it would provide for the benefits and advantage of having a centralized entity to manage and control of all identification and credentials services (*Col 5, lines 48-64*)

Claims 11, 13, 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fraser, and further in view of Yoon et al (US 6,088,794, hereinafter Yoon).

Regarding claim 11, Fraser discloses the remote access system according to claim 10 wherein the storage medium stores an OS program to be used to drive the client device (*Fig. 1, element 32; Col 11, lines 41-52; Col 12, lines 12-20, wherein the OS program stored in the smartcard reader is used to drive the client device*),

Fraser does not disclose a switch is provided to set whether to drive the client device by using the OS program or drive the client device without using the OS program.

However, Yoon discloses a switch is provided to set whether to drive the device by using the OS program or drive the device without using the OS program. (*Fig 2, Col 6, lines 19-24,* *50-54; Fig 3, element 21; Col 6, lines 55-67; Col 7, lines 1-5, wherein a switch unit in a selective booting function is used to select different OS program to boot the system*)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Yoon into the teachings of Fraser because it would provide for an improved computer system capable of selective booting from multiple disk drives. (*Col 1, lines 39-52; Col 2, lines 32-35*)

Regarding claim 13, Fraser discloses the remote access system according to claim 11 (*Fig. 1, element 32; Col 11, lines 41-52; Col 12, lines 12-20, wherein the OS program stored in the smartcard reader is used to drive the client device*),

Fraser does not disclose when it is set in the switch to drive the client device without using the OS program stored in the storage medium, the client device acquires the setting from the storage medium, executes an OS program previously stored in the client device instead of the OS program stored in the storage medium, and conducts the driving.

It is obvious to one of ordinary skill in the art that the client device acquires the setting from the storage medium in order to get access to the storage medium under the selected operating system.

However, Yoon discloses when it is set in the switch to drive the client device without using the OS program stored in the storage medium, executes an OS program previously stored in the client device instead of the OS program stored in the storage medium, and conducts the driving (*Fig 6, elements S32-S37, Col 10, lines 36-55, wherein when a determination is made to boot the first hard disk drive, the first hard disk drive is reset, following a booting operation is* *performed from the first hard disk drive. When the first hard disk drive is not selected, the second hard disk drive is reset, and booting from the second hard disk drive operation is performed.*

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Yoon into the teachings of Fraser because it would provide for an improved computer system capable of selective booting from multiple disk drives. (*Col 1, lines 39-52; Col 2, lines 32-35*)

Regarding claim 14, Fraser discloses the remote access system according to claim 10, wherein

the storage medium is connected to the client device via a reader/writer of the storage medium (*Col 10, lines 12-16, wherein communication between smartcard which corresponds to storage medium and client device is through the I/O controller of the reader*), and

the storage medium stores an OS program to be used to drive the client device (*Col 8, lines 64-67; Col 9, lines 1-6; Col 12, lines 12-16, wherein an OS program is used to drive the client device)*, and

Fraser does not disclose the reader/writer comprises a switch to set whether to drive the client device by using the OS program or drive the client device without using the OS program.

However, Yoon discloses a switch is provided to set whether to drive the device by using the OS program or drive the device without using the OS program. (*Fig 2, Col 6, lines 19-24,* *50-54; Fig 3, element 21; Col 6, lines 55-67; Col 7, lines 1-5, wherein a switch unit in a selective booting function is used to select different OS program to boot the system*)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Yoon into the teachings of Fraser because it would provide for an improved computer system capable of selective booting from multiple disk drives. (*Col 1, lines 39-52; Col 2, lines 32-35*)

Claims 15, 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fraser, and further in view of Golding et al (US 5,265,163, hereinafter Golding).

Regarding claim 15, Fraser discloses the remote access system according to claim 9, wherein the client device (*Fig. 1, element 14; Col 7, lines 30-31; Col 8, line 38; terminal or computer*);

stores an OS program to be used to drive the client device, in a storage device provided in the client device (*Fig 1, element 30, client software*);

executes a boot program stored in the storage medium *(Col 12, lines 12-20; Col 15, lines 6-21 wherein boot program from the smartcard is executed)* ; and

authentication information stored in the storage medium (*Col 9, lines 7-9, wherein private key which corresponds to authentication information is stored on the smartcard*)

Fraser does not disclose access restriction is set in the storage device provided in the client device, and

when the access restriction is set and the access restriction can be canceled, the client device is driven by canceling the access restriction and executing the OS program stored in the storage device .

However, Golding discloses access restriction is set in the storage device provided in the client device (*Col 2, lines 18-27, wherein a password from the user is required before accessing is granted)*, and

when the access restriction is set and the access restriction can be canceled (*Col 2, lines 18-27, wherein when the correct password from the user is entered, access to computer functions is granted, thus access restriction is canceled*), the client device is driven by canceling the access restriction and executing the OS program stored in the storage device (*Col 2, lines 18-27, wherein once access is granted, the system is permitted to boot using the OS program stored in the storage device*).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Golding into the teachings of Fraser because it would provide for the prevention of contamination by computer viruses (*Col 1, lines 59-68; Col 2, lines 1-15*).

Regarding claim 16, Fraser discloses the remote access system according to claim 15, wherein the storage medium stores an OS program to be used to drive the client device (*Col 8, lines 64-67; Col 9, lines 1-6; Col 12, lines 12-16, wherein an OS program is used to drive the client device)*, and

the client device is driven by executing the OS program stored in the storage medium *(Col 12, lines 12-20; Col 15, lines 6-21 wherein boot program from the smartcard is executed)*

Fraser does not disclose when the access restriction cannot be canceled

However, Golding discloses when access restriction cannot be canceled (*Col 2, lines 18-27, wherein a password from the user is required prior to access is granted to boot the system, so if the incorrect password is entered, access will not be granted, thus, the access restriction cannot be canceled*)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Golding into the teachings of Fraser because it would provide for the prevention of contamination by computer viruses (*Col 1, lines 59-68; Col 2, lines 1-15*).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to PHY ANH VU whose telephone number is (571)270-7317. The examiner can normally be reached on Mon-Thr 7:30-5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Thomas Pham can be reached on 571-272-3689. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

PVU

/THOMAS PHAM/
Supervisory Patent Examiner, Art Unit 4148